(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平11－164132

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]	識別記号	FI		
H04N	1/387	H04N	1/387	
G06T	1/00	G09C	5/00	
G09C	5/00	G06F	15/66	B
H04N	5/91	H04N	5/91	P
// H04L	9/36	H04L	9/00	685

審査請求　有　請求項の数31　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－143705

(22)出願日　平成10年(1998)５月26日

(31)優先権主張番号　特願平9－248272

(32)優先日　平９(1997)９月12日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　三和　邦彦
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

(74)代理人　弁理士　坂口　博　（外１名）

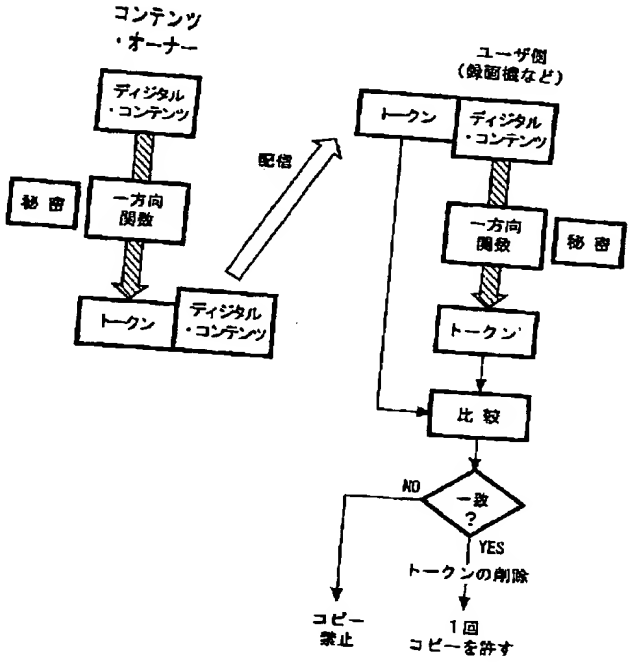
最終頁に続く

(54)【発明の名称】　データ制御システム

(57)【要約】

【課題】電子透かし技術を用いて、製造コストが低く、安全にデータ制御を行うシステムおよびその方法を提供することである。

【解決手段】電子透かし技術により、データの制御を行うことを示すコントロール・フラグを、データに埋め込み、データをどのように制御するかの情報を有するトークン、を前記データの内容を用いて作成し、前記トークンを前記データに付加して配信し、配信されたデータから、前記コントロール・フラグを検出し、前記コントロール・フラグが検出された場合、前記データに付加された前記トークンを読みだし、前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う、データ制御システムを構築する。また、データの制御時に、トークンの変更操作により、以後のデータ制御をさらに抑制できる。



【特許請求の範囲】

【請求項１】データ制御システムであって、該システムが、

電子透かし技術により、データ制御を行うことを示す、コントロール・フラグを、配信するデータに埋め込む手段と、

データをどのように制御するかの情報を有するトークンを、前記データの内容を用いて作成する手段と、

前記トークンを前記データに付加する手段と、

前記トークンの付加された前記データを配信する手段と、

配信されたデータから、前記コントロール・フラグを検出する手段と、

前記コントロール・フラグが検出された場合、前記データに付加された前記トークンを読みだす手段と、

前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う手段と、

を具備する、データ制御システム。

【請求項２】前記データの制御を行う手段が、さらに前記トークンを変更、無効化、若しくは削除する手段を含む、請求項１記載のシステム。

【請求項３】前記制御が、複製制御、再生制御、若しくは受信制御である、請求項２記載のシステム。

【請求項４】データ複製装置であって、該装置が、

データから、該データに電子透かし技術により埋め込まれた、データの複製制御を行うことを示す、コントロール・フラグを検出する手段と、

前記コントロール・フラグが検出された場合、前記データから、データの複製制御情報を示す、トークンを読みだす手段と、

前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの複製制御を行う手段と、

を具備する、データの複製装置。

【請求項５】データ再生装置であって、該装置が、

データから、該データに電子透かし技術により埋め込まれた、データの再生制御を行うことを示す、コントロール・フラグを検出する手段と、

前記コントロール・フラグが検出された場合、前記データから、データの再生制御情報を示す、トークンを読みだす手段と、

前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの再生制御を行う手段と、

を具備する、データ再生装置。

【請求項６】データ受信装置であって、該装置が、

データから、該データに電子透かし技術により埋め込まれた、データの受信制御を行うことを示す、コントロール・フラグを検出する手段と、

前記コントロール・フラグが検出された場合、前記データから、データの受信制御情報を示す、トークンを読みだす手段と、

前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの受信制御を行う手段と、

を具備する、データの受信装置。

【請求項７】データ制御装置であって、該装置が、

データから、該データに電子透かし技術により埋め込まれた、データの制御を行うことを示す、コントロール・フラグを、検出する手段と、

前記コントロール・フラグが検出された場合、前記データから、データをどうように制御するかを示す、トークンを読みだす手段と、

前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う手段と、

を具備する、データ制御装置。

【請求項８】データ制御を行うためのトークンを作成するトークン作成装置であって、該装置が、

電子透かし技術により、データの制御を行うことを示すコントロール・フラグを、データに埋め込む手段と、

データをどのように制御するかの情報を有するトークンを、前記データの内容を用いて作成する手段と、

前記トークンを前記データに付加する手段と、

を具備する、トークン作成装置。

【請求項９】データ制御システムであって、該システムが、

電子透かし技術により、データの制御を行うことを示す、コントロール・フラグを、配信するデータに埋め込む手段と、

データをどのように制御するかの情報を有するトークンを、前記データの内容を用いて作成する手段と、

前記トークンを前記データに付加する手段と、

前記トークンの付加された前記データを配信する手段と、

配信されたデータから、前記コントロール・フラグを検出する手段と、

前記コントロール・フラグが検出された場合、前記データに付加されたトークンを読みだす手段と、

前記データから再度、トークンを作成する手段と、

読みだされたトークンと、再度作成されたトークンを比較する手段と、

前記比較が一致した場合、前記読みだされたトークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う手段と、

を具備する、データ制御システム。

【請求項１０】前記データの制御を行う手段が、さらに前記付加されたトークンを削除する手段を含む、請求項９記載のシステム。

【請求項１１】前記トークンを作成する手段、および前記再度トークンを作成する手段が、さらに一方向関数を用いて、データからトークンを作成する手段を含む、請求項１０記載のシステム。

【請求項１２】前記制御が、複製制御、再生制御、若しくは受信制御である、請求項１１記載のシステム。

【請求項１３】データ複製装置であって、該装置が、
データから、該データに電子透かし技術により埋め込まれた、データの複製制御を行うことを示す、コントロール・フラグを検出する手段と、
前記コントロール・フラグが検出された場合、前記データから、データの複製制御情報を示す、トークンを読みだす手段と、
前記データから、トークンを作成する手段と、
読みだされたトークンと、作成されたトークンを比較する手段と、
前記比較が一致した場合、前記読みだされたトークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、複製に関する、前記データの制御を行う手段と、
を具備する、データ複製装置。

【請求項１４】データ再生装置であって、該装置が、
データから、該データに電子透かし技術により埋め込まれた、データの再生制御を行うことを示す、コントロール・フラグを検出する手段と、
前記コントロール・フラグが検出された場合、前記データから、データの再生制御情報を示す、トークンを読みだす手段と、
前記データから、トークンを作成する手段と、
読みだされたトークンと、作成されたトークンを比較する手段と、
前記比較が一致した場合、前記読みだされたトークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、再生に関する、前記データの制御を行う手段と、
を具備する、データ再生装置。

【請求項１５】データ受信装置であって、該装置が、
データから、該データに電子透かし技術により埋め込まれた、データの受信制御を行うことを示す、コントロール・フラグを検出する手段と、
前記コントロール・フラグが検出された場合、前記データから、データの受信制御情報を示す、トークンを読みだす手段と、
前記データから、トークンを作成する手段と、
読みだされたトークンと、作成されたトークンを比較する手段と、
前記比較が一致した場合、前記読みだされたトークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、受信に関する、前記データの制御を行う手段と、
を具備する、データ受信装置。

【請求項１６】データの制御を行うデータ制御装置であって、該装置が、
データから、該データに電子透かし技術により埋め込まれた、データも制御を行うことを示す、コントロール・フラグを、検出する手段と、
前記コントロール・フラグが検出された場合、前記データから、データをどうように制御するかを示す、トークンを読みだす手段と、
前記データから、トークンを作成する手段と、
読みだされたトークンと、作成されたトークンを比較する手段と、
前記比較が一致した場合、前記読みだされたトークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う手段と、
を具備する、データ制御装置。

【請求項１７】前記データを制御する手段が、さらに前記付加されたトークンを削除する手段を含む、請求項１３乃至請求項１６の何れかに記載の装置。

【請求項１８】データ制御を行うためのトークンを作成するトークン作成装置であって、該装置が、
電子透かし技術により、データの制御を行うことを示すコントロール・フラグを、データに埋め込む手段と、
データをどのように制御するかの情報を有するトークンを、前記データの内容を用いて作成する手段と、
前記トークンを前記データに付加する手段と、
を具備する、トークン作成装置。

【請求項１９】前記トークンを作成する手段が、さらに一方向関数を用いて、データからトークンを作成する手段を含む、請求項１３乃至請求項１８の何れかに記載の装置。

【請求項２０】データ制御方法であって、
電子透かし技術により、データの制御を行うことを示す、コントロール・フラグを、配信するデータに埋め込むステップと、
データをどのように制御するかの情報を有するトークンを、前記データの内容を用いて作成するステップと、
前記トークンを前記データに付加するステップと、
前記トークンの付加された前記データを配信するステップと、
配信されたデータから、前記コントロール・フラグを検出するステップと、
前記コントロール・フラグが検出された場合、前記データに付加された前記トークンを読みだすステップと、
前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行うステップと、
を有する、データ制御方法。

【請求項２１】前記データの制御を行うステップが、さらに前記トークンを変更、無効化、若しくは削除するス

テップを含む、請求項２０記載の方法。
【請求項２２】前記制御が、複製制御、再生制御、若しくは受信制御である、請求項２１記載の方法。
【請求項２３】データの制御を行わせるためのプログラムを含む媒体であって、該プログラムが、
データから、該データに電子透かし技術により埋め込まれた、データの制御を行うことを示す、コントロール・フラグを、検出する機能と、
前記コントロール・フラグが検出された場合、前記データから、データをどうように制御するかを示す、トークンを読みだす機能と、
前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う機能と、
を有することを特徴とする、プログラムを含む媒体。
【請求項２４】データ制御を行うためのトークンを作成するためのプログラムを含む媒体であって、該プログラムが、
電子透かし技術により、データの制御を行うことを示すコントロール・フラグを、データに埋め込む機能と、
データをどのように制御するかの情報を有するトークンを、前記データの内容を用いて作成する機能と、
前記トークンを前記データに付加する機能と、
を有することを特徴とする、プログラムを含む媒体。
【請求項２５】デジタル・コンテンツの複製制御を行うトークン作成装置であって、該トークン作成装置が、
電子透かし技術により、デジタル・コンテンツの複製を許可することを示す、コントロール・フラグを、デジタル・コンテンツに埋め込む手段と、
前記デジタル・コンテンツの複製制御を行う情報を有するトークンを、前記デジタル・コンテンツから、１方向関数を用いて作成する手段と、
前記トークンを前記デジタル・コンテンツに付加する手段と、
を具備する、トークン作成装置。
【請求項２６】デジタル・コンテンツの複製装置であって、
デジタル・コンテンツから、該デジタル・コンテンツに電子透かし技術により埋め込まれた、デジタル・コンテンツの複製を許可することを示す、コントロール・フラグを検出する手段と、
前記コントロール・フラグが検出された場合、前記デジタル・コンテンツに、付加されたトークンを読みだす手段と、
前記デジタル・コンテンツから、１方向関数を用いて、トークンを作成する手段と、
読みだされたトークンと、作成されたトークンを比較する手段と、
前記比較が一致した場合、前記デジタル・コンテンツの複製を行う手段と、
次回のトークン比較が失敗するように、前記デジタル・コンテンツから前記付加されたトークンを削除するか、若しくは前記デジタル・コンテンツを変更する手段と、
を具備する、デジタル・コンテンツの複製装置。
【請求項２７】データ制御装置であって、該装置が、
データから、該データに電子透かし技術により埋め込まれた、データの制御を行うことを示す、コントロール・フラグを検出する手段と、
前記コントロール・フラグが検出された場合、前記データから、データの制御情報を示す、トークンを読みだす手段と、
外部からの入力情報に基づき、前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う手段と、
を具備する、データ制御装置。
【請求項２８】データ制御装置であって、該装置が、電子透かし技術により埋め込まれたデータの制御を行うことを示す、コントロール・フラグ及び、データの制御情報を示すトークンを含むデータを受け取る手段と、
外部からの入力情報に基づき、前記トークン若しくは前記コントロール・フラグの予め定義された制御ルールに従って、前記データの制御を行う手段と、
を具備する、データ制御装置。
【請求項２９】前記制御が、複製制御、再生制御、若しくは受信制御である、請求項２７乃至２８の何れかに記載のシステム。
【請求項３０】前記データの制御を行う手段が、前記トークンを破壊若しくは、前記トークンを無効にする手段を含む、請求項２７乃至２８の何れかに記載のシステム。
【請求項３１】前記外部からの入力が、課金情報若しくはユーザ入力情報である、請求項２７乃至２８の何れかに記載のシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、電子透かし技術を用いた、データ制御システムに関する。より具体的には、データの制御を行うことを示すコントロール・フラグ、およびデータをどのように制御するかの情報を有するトークンを用いて、前記データが配信先において、所望のデータ制御（例えば複製制御、再生制御、受信制御等）が行えるようにする技術に関する。
【０００２】
【従来の技術】マルチメディア環境が普及するに従い、問題となるのが著作物の保護である。デジタル・ビデオ・ディスク（ＤＶＤ）、セットトップボックス（ＳＴＢ:Set Top Box）、ケーブルテレビ（Cable TV)、ネットワーク配信等は、劇場用映画等の配布に十分なハード・ウェア的な仕様を有するにもかかわらず、これらのコンテンツの保護、特に不法な複製（コピー）の問題に関

しては、コンテンツの供給者が十分に納得できるような仕様が提供されていない。デジタル・データは、データ内容の複製、改変が極めて容易であるにもかかわらず、それらを防ぐ有効な仕様が提供されていないからである。本発明では、１回のみコピーを許す（onetime copy）等の条件付きの配布が行えるように、コンテンツ自信に制御の仕組みを組み込むことができる方法を用いて、これらの媒体（メディア）を用いた多数の魅力的なコンテンツの配布を、安全に行う仕組みを提供する。従来行われたきた、コンテンツ保護、複製禁止、再生禁止等を行うデータ制御の方法は幾つか存在する。例えば、特開平 6-4026 では、各カテゴリーの許可情報を示すコードとして、適当に生成したコード１に一方向性の変換ｆを行ったコード２を生成し、許可を示す時は、コード１とコード２を併記し、禁止を示すときは、コード２のみを記述することにより、許可状態のコード作成を困難にする技術が開示されている。しかしながら、このような方法では、コード１を保存しておいて後から再併記することにより、コピーを再度行なうことが出来る。

【０００３】例えば、特開平 6-309239 では、データファイルがコピーされていないことを示すフラグファイルを用いて、該フラグファイルが存在すれば暗号化したデータファイルを本来のデータファイルに変換し、データファイルのコピー後に該フラグファイルを削除する、１回のみコピーを許可する方法を開示している。しかしながら、この方法では、フラグファイルがデータファイルと別ファイルであるため、フラグファイルを保存し、再現するだけで容易に再度のコピーが可能である。また、フラグの不一致や存在なき場合に複製禁止と判断してしまうため、自分で撮影したり製作したコンテンツまで禁止のカテゴリーに入ってしまう。

【０００４】従来の方法は、基本的にデータ制御を行うにあたり、そのデータとは別のコード、フラグ等を用いている。このような方法では、その別のコードや、フラグが特定されれば、これを操作することが可能であり、悪意を持った第３者の攻撃に弱い。このような欠点を持たない、データ制御に用いることのできる技術が望まれる。さらに、従来技術におけるデータ制御の方法と、完全に独立したデータ制御方法であって、既存の映像の配布システムやデバイスの仕組みに影響を与えることのない、上位互換（upper compatible）または下位互換（downward compatible）な、新しいデータ制御を行う方法が望まれる。

【０００５】静止画像や動画像、音声の著作権保護の為の技術として、電子透かし技術（ウォーターマーク技術：Watermarking）がある。電子透かし技術とは、データハイディング(TM)技術とも呼ばれる技術である。簡潔に言えば、ある情報を他の媒体（静止画像、音声、動画など）に埋め込むための技術の総称であり、この技術のめざすところは、暗号化と異なり、どう情報を秘匿するかではなく、どう情報を埋め込む対象の媒体と一体化するかにある。というのは、隠したい情報を、媒体のデータ中に埋め込むにあたり、その媒体のデータを操作することにより前記情報を埋め込む方法を採るからである。例えば画像データでは、輝度等の画素値を変更して本来のデータ以外の情報を持たせる事を意味する。なお、本発明において「埋め込み」とは、電子透かし技術等を用いて、追加の情報をデータ自身の変形という形で隠蔽することを意味する。

【０００６】電子透かしの大きな特徴の１つとして、非可視または非可聴のマーキング手法である点が挙げられる。メディアに対して情報を埋め込む際に、データ・ビットを追加するのではなく、既存のデータを人間の視覚で検知できないように加工（データ変形）して情報を埋め込むため、付加情報の埋め込みによる総データ量の増加がない。たとえば、640 x 480 画素を持つ画像にデータを埋め込んでも 640x 480 画素には変わりはない。またテキスト情報や音声情報を画像に埋め込むことにより、ストレージ側では一種類の媒体だけを取り扱えば良いことになる。最も大きな特徴の１つとして、埋め込み情報の不可分性が挙げられる。電子透かしは、付加情報をヘッダや別ファイルではなく、媒体のデータ構造に直接埋め込むため、媒体のプラットフォームやデータ・フォーマットが変わっても、元データの品質が保存されている限り、埋め込んだ情報を取り出すことができる。

【０００７】この電子透かし技術を用いた、データ制御方法の１例を以下に示す。なおデータの配信先での録画、複製、再生に限らず、電波などによるデータの配信において、該データの受信を許可するか否かの制御（受信制御）も全く同様に可能である。

（１）電子透かし技術を用いてコンテンツの保護レベルを示すコントロール・フラグ（Control flag：ＣＦ）を画像データ内に埋め込むステップ。

（２）録画および再生装置において、前記コンテンツに埋め込まれたＣＦを検出し、録画または再生の可否を判断し、適宜録画または再生の制御を行うステップ。（録画の場合、録画禁止を示すＣＦが検出された場合に録画を停止する、再生の場合、再生媒体が録画用で、かつ、録画禁止を示すＣＦが検出された場合は、違法コピーと判断し、再生を停止する）

（３）１回のみ録画可を示すＣＦが検出された場合は、録画を許可し、かつ録画されたことを示す記録を残す。この録画されたコンテンツを再生し、再度の録画を試みた場合、ＣＦと録画済みマークから、再度の録画を阻止するステップ。

【０００８】ここで（１）および（２）のステップについては、コンテンツの作成時に電子透かし技術により、事前にコンテンツにＣＦを埋め込むことにより実現することができる。（３）のステップについても、（１）、（２）のステップ同様電子透かし技術を用いて再度の録

画禁止を実現することはできる。しかしこの場合は問題が生じる。録画装置は通常、エンドユーザが所有していることが多く、コンパクトでしかも廉価に作成されなければならない。このような限られた処理能力の装置の中で、コンテンツ作成時のように、画質や残存信号強度に配慮した、録画済みマークを付加する、電子透かし埋め込みを実行することは現実的に難しい。

【０００９】例えば対象となる画像データがＭＰＥＧ圧縮された画像データである場合、ＣＦの検出を行うためのビデオデータの分離機能のほかに、録画済みマークの埋め込みを施した後の画像データを残りのデータ（音声データやサブピクチャなど）と再合成して戻す機能が必要となる。このためのバッファや回路を合計すると、ＣＦの検出回路の２倍以上となり、現実的な解決策とはならない。さらに、埋め込みの対象となるビデオデータはI-frame のみとなるため、ＭＰＥＧの解凍が行われたときに、埋め込んだ情報が他のフレーム（ＢとＰ）に残らないという欠点がある。

【００１０】

【発明が解決しようとする課題】従って、本発明が解決しようとする課題は、電子透かし技術を用いて、製造コストが低く、安全にデータ制御を行うシステムおよびその方法を提供することである。

【００１１】また別の課題は、電子透かし技術を用いて、安全にデータの複製制御、再生制御、若しくは受信制御を行うシステムを提供することである。

【００１２】また別の課題は、悪意を持った第３者の攻撃に耐えられるデータ制御の方法およびシステムを提供することである。

【００１３】また別の課題は、従来技術と比較して、コスト的に安価で、機能的に同等かそれ以上の効果を得られる、データ制御の方法およびそのシステムを提供することである。

【００１４】また別の課題は、従来技術におけるデータ制御の方法と、完全に独立したデータ制御方法であって、既存の方法と共存できる、新しいデータ制御を行う方法及びそのシステムを提供することである。

【００１５】

【課題を解決するための手段】上記課題を解決するために、電子透かし技術により、データの制御を行うことを示すコントロール・フラグを、データに埋め込み、データをどのように制御するかの情報（例えば、複製回数、再生回数、再生機器の指定、ユーザの指定等）を有するトークン、を前記データの内容を用いて作成し、前記トークンを前記データに付加して配信し、配信されたデータから、前記コントロール・フラグを検出し、前記コントロール・フラグが検出された場合、前記データに付加された前記トークンを読みだし、前記トークン若しくは前記コントロール・フラグの予め定義された制御ルール（トークン、各種フラグ、メディアの種類を含む組み合わせにより制御の種類を決める規則）に従って、前記データの制御を行う、データ制御（複製制御、再生制御、受信制御を含む）システムを構築する。また、データの制御時に、トークンの変更操作（トークンの削除、トークンの無効化、トークン数の増減、トークン作成用画像部の変更）により、以後のデータ制御をさらに抑制できる。

【００１６】

【発明の実施の形態】トークン作成とデータ制御の２つに分けて説明する。まず図７にトークン作成の処理の流れを示す。ステップ７００において、電子透かし技術を用いてオリジナルのデータにＣＦを埋め込む。ここでデータとは画像、音声、静止画、動画等を指す。次にステップ７１０において、ＣＦの埋め込まれたデータにおいてトークン作成対象となる部分を埋込み鍵を用いて抽出する。抽出した部分データから、ステップ７２０で一方向関数を用いてトークンを作成する。なお１方向関数を用いる他に、要約から非対称鍵で作成する方法を用いてもよい。その他、例えばトークンを異なる鍵を用いて複数作成してもよい。そしてステップ７３０で、ＣＦの埋め込まれたデータに作成したトークンを付加する。この時、例えばユーザ・データ領域を使用して付加する。

【００１７】次にデータ制御の処理の流れを図８に示す。まずステップ８００において、配信されたデータから電子透かし技術を用いて埋め込まれたＣＦがあるかどうかを調べる。ステップ８００でＣＦが検出されなければ何も、制限のない制御、例えば複製、録画、又は再生等が行われる。ステップ８００でＣＦが検出されると、次にステップ８２０で付加されたトークンがあるかどうかを判断する。（この時、トークンの検証を含めてもよい。）もしステップ８２０の結果がＮＯであれば、データ制御は禁止される。すなわち複製、録画、又は再生等は行われず、そのまま終了となる。もしステップ８２０の結果がＹＥＳであれば、トークン若しくは前記コントロール・フラグの予め定義された制御ルールによるデータ制御（複製、録画、又は再生等）が行われる。ここで予め定義された制御ルールとは、トークンやフラグの他、データを記憶、再生するメディアの種類等により、その制御内容を定義した規則である。通常はテーブル化した各パラメータの組み合わせでその制御内容を決める。なおこのような組み合わせ方法は既知であるので本願では詳細に触れない。当業者であれば該規則をより詳細にして、その他、種々の制御の実施が行えるよう容易に変形できる。 必要であればステップ８４０で、その後のデータ制御を変更するためにトークンの操作を行う。トークンの操作とは、複製回数を制限するためのトークン数の増減、削除、無効化、変更を意味している。その他トークン作成対象となる部分データの操作を行ってもよい。なお上記トークンの操作は、安全性のためにトークンによるデータ制御を行う前に行ってもよい。

【００１８】なお、コントロール・フラグとトークンの役割の違いは、コントロール・フラグが存在する時のみ、予め決められたデータ制御が行われる事を意味する以外、違いはない。つまり、コントロール・フラグにデータを制御する情報（複製を許可する回数など）を持たせても良いし、トークンに持たせても良いし、両方に持たせてもよい。

【００１９】

【実施例】以下、図面を参照して本発明の実施例を説明する。図１には、本発明において使用されるデータ制御（複製制御、再生制御、受信制御、トークン作成を含む）システムのハードウェア構成の一実施例を示す。システム１００は、中央処理装置（ＣＰＵ）１とメモリ４とを含んでいる。ＣＰＵ１とメモリ４は、バス２を介して、補助記憶装置としてのハードディスク装置１３（またはMO、ＣＤ－ＲＯＭ２３、ＤＶＤ３２等の記憶媒体駆動装置）とＩＤＥコントローラ２５を介して接続してある。同様にＣＰＵ１とメモリ４は、バス２を介して、補助記憶装置としてのハードディスク装置３０（またはＭＯ２８、ＣＤ－ＲＯＭ２３、ＤＶＤ３１等の記憶媒体駆動装置）とＳＣＳＩコントローラ２７を介して接続してある。フロッピーディスク装置２０はフロッピーディスクコントローラ１９を介してバス２へ接続されている。

【００２０】フロッピーディスク装置２０には、フロッピーディスクが挿入され、このフロッピーディスク等やハードディスク装置１３（またはMO、ＣＤ－ＲＯＭ、ＤＶＤ等の記憶媒体）、ＲＯＭ１４には、オペレーティングシステムと協働してＣＰＵ等に命令を与え、本発明を実施するためのコンピュータ・プログラムのコード若しくはデータを記録することができ、メモリ４にロードされることによって実行される。このコンピュータ・プログラムのコードは圧縮し、または、複数に分割して、複数の媒体に記録することもできる。

【００２１】システム１００は更に、ユーザ・インターフェース・ハードウェアを備え、入力をするためのポインティング・デバイス（マウス、ジョイスティック等）７またはキーボード６や、視覚データをユーザに提示するためのディスプレイ１２を有することができる。またパラレルポート１６を介してプリンタを接続することや、シリアルポート１５を介してモデムを接続することが可能である。このシステム１００は、シリアルポート１５およびモデムまたは通信アダプタ１８(イーサネットやトークンリング・カード)等を介してネットワークに接続し、他のコンピュータ等と通信を行うことが可能である。本発明では、フロッピーディスク等の媒体によるデータの配信を行う他に、配信データをシリアルポート１５およびモデムまたは通信アダプタ１８により送受信することもできる。またシリアルポート１５若しくはパラレルポート１６に、遠隔送受信機器を接続して、赤外線若しくは電波等によりデータの送受信を行ってもよい。

【００２２】スピーカ２３は、オーディオ・コントローラ２１によってＤ／Ａ（デジタル／アナログ変換）変換された音声信号を、アンプ２２を介して受領し、音声として出力する。また、オーディオ・コントローラ２１は、マイクロフォン２４から受領した音声情報をＡ／Ｄ（アナログ／デジタル）変換し、システム外部の音声情報をシステムにとり込むことを可能にしている。

【００２３】このように、本発明のデータ制御システム１００は、通常のパーソナルコンピュータ（ＰＣ）やワークステーション、ノートブックＰＣ、パームトップＰＣ、ネットワークコンピュータ、コンピュータを内蔵したテレビ等の各種家電製品、通信機能を有するゲーム機、電話、ＦＡＸ、携帯電話、ＰＨＳ、電子手帳、等を含む通信機能有する通信端末、または、これらの組合せによって実施可能であることを容易に理解できるであろう。ただし、これらの構成要素は例示であり、その全ての構成要素が本発明の必須の構成要素となるわけではない。

【００２４】トークン作成及びデータ制御を行う、ＤＶＤ－Ｒシステムの実施例を説明する。図１のシステム１００のＤＶＤ３１若しくはＤＶＤ３２を外部接続した場合を図２に、内蔵した場合を図３に示す。外付け型ＤＶＤ－Ｒドライブ４０および内蔵型ＤＶＤ－Ｒドライブ５０は、ＩＤＥ（ＡＴＡＰＩ：ATA Packet Interface）インターフェースによりシステム１００と接続される（なおＳＣＳＩ経由でも可能）。該ＤＶＤ－Ｒシステムのブロック図を図４に示す。

【００２５】図４において、ディスク２１０はドライブ回路２１２に接続されたモータ２１４により回転し、ディスク２１０中に記録されたデータはオプトエレクトリカル・ヘッド２１６により読み取られる。またドライブ回路２１２はＤＶＤ制御ブロック２１８からの指令で動作する。オプトエレクトリカル・ヘッド２１６により読み取られた信号は、ＤＶＤ制御ブロック２１８に入力され、増幅され、必要に応じて変換され、復号ブロック２２０へ送られる。複合ブロック２２０は信号のモジュレータ、デモジュレター及び誤り訂正を行う。ＤＶＤ制御ブロック２１８はディスク中に記録されたサーボデータまたは復号ブロックからの制御信号を受けてドライブ回路２１２を制御するためのサーボ回路２１８Ｂを含んでいる。またＤＶＤ制御ブロック２１８は信号読取回路２１８Ａを含んでいる。

【００２６】復号ブロック２２０で受け取られたデータは、共通のバスで接続された復号ブロック内にあるバッファ２２０Ａ、ＭＰＵ２２０Ｂ及び復号器２２０Ｃにより誤り訂正を行い、リアルタイムに復号され、データ制御ブロック２３０へ送信される。データ制御ブロック２３０では、電子透かし技術による、ＣＦ情報の埋め込

み、トークンの生成、トークンの対象データへの付加、ＣＦ情報の検出、トークンによるデータ制御、及びトークンの操作が行われる。データ制御ブロック２３０から、映像データはＡＴＡＰＩインターフェース２２２を介してシステム１００へ、音声データはＤＡＣ（デジタルアナログ・コンバータ）２２４を介してシステム１００へそれぞれ送られる。

【００２７】記録する場合は、データはＡＴＡＰＩインターフェース２２２からデータ制御ブロック２３０、複合ブロック２２０、そしてＤＶＤ制御ブロックの順に、読み取り時と逆に流れる。またこの時オプトエレクトリカル・ヘッド２１６は記録ヘッドとして動作する。なお上記ＤＶＤ－Ｒデータ制御システムは、データ処理システム１００との協働によるものであるが、単体のＤＶＤ再生機、ＤＶＤ－Ｒ録画機でも同様に、本発明の本質を外れることなく実施可能である。

【００２８】図５に１方向ハッシュ関数を利用したディジタル画像配信における複製制御システムの実施例を示す。概要的には、電子透かし技術を用いて、放送されるデジタルデータに複製や記録を制御する“トークン”を付加し、複製または記録されると同時に、この“トークン”を無効にすることにより更なる複製または記録ができないようにするシステムである。なおトークンにはＣＦ（コントロール・フラグ）と同様に、データをどのように制御するかの情報（例えば、複製を許す回数、再生を許す回数、再生機器の指定、ユーザの指定等）を含めることができるが、簡潔に説明するため、図５、図６ではトークンの存在の有り無しにより、データ複製の可否を判定することとする。またトークンの数は実施環境の違いに応じて所望の数に増減できる。（例えばトークンの数を複製回数、再生回数の限界と定義してもよい。）

【００２９】図５の実施例では、コンテンツに１回までのコピーを可能とすることを示すＣＦを電子透かし技術によって埋め込んでおく。このＣＦが検出された時のみ、録画機は１回のみのコピーを可能とする。デジタル画像、デジタルビデオ、デジタルオーディオなどのデジタル・コンテンツ（ＭＰＥＧなどの圧縮後のストリームも含む）に、コンテンツの内容を演算した結果を付加する。なおこの演算結果を“トークン”と呼ぶ。この“トークン”の存在があるかないかで、複製または記録の可否を判定する。

【００３０】より詳細に複製制御システムを説明する。図５においてトークンは、１方向ハッシュ関数などを用いて、画像データの一部（またはすべて）から計算されたビット列とし、コメントフィールドやユーザデータとして所定の場所に記録、保持し画像データとともに配信する。トークンの作成するのに用いる１方向性ハッシュ関数は、一般的に知られるもので例えば、ＭＤ５やＣＲＣ(Cyclic RedundancyCheck)などが使用できる。トークンを作成する関数や、画像のどの部分を対象として演算しているかは秘密とし、ユーザ側においてトークンを生成することができない様にする。

【００３１】１方向ハッシュ関数の対象となる画像データは、埋め込み鍵により選択される。画像データのどの部分が使用されるかと、ハッシュ演算の初期値が秘密であり、ハッシュ関数自体は公開されているものを使用する。作成されたトークンは、伝送される画像の付加データ領域（例えばＭＰＥＧ２の場合は、ユーザ・データ領域―８ビット単位で８ ｘ ｎビット使用可）に記録することでトークンの付加を行う。１方向ハッシュ関数は、一般的に下記の様に表現される。ｈ＝Ｈ（Ｍ）ここで、Ｍは任意の長さのメッセージ（数値）で、ｈは固定長の数値で、Ｈは定義されたハッシュ関数である。１方向ハッシュ関数は、上記の条件以外に、以下の条件を満たすとして定義される。・Ｍが与えられたときにｈを計算することが容易であること。・ｈが与えられたときにＭを計算する（逆変換）ことが困難であること。・Ｍが与えられたとき、Ｈ（Ｍ）=Ｈ（Ｍ’）を満たすＭ’を見つけることが困難であること。この特性を利用して、データに電子的に署名を施し、認証を行ったり、改ざんの有無を検出することに利用する。入力のメッセージＭは、複数要素でも可であり、ここでは、以下の方法でハッシュを作成する例をあげる。

$H_i = H(I^i, h^{i-1})$　　$(I^0 = k)$

つまり、M^iを$I^1, I^2 \ldots I^n$とｉ番めまでのハッシュ値の組み合わせとした。ここで、I^iは画像データ・ブロックで、埋め込み鍵により、I^1からI^nまでｎ個選択される。H_iは、Ｉ番目の画像データ・ブロックのハッシュ値で、I^iとI^{i-1}番めまでのハッシュ値（h^{i-1}）を入力として求められ、この演算は対象となる画像データ・ブロックの数（ｎ）だけ繰り返されて、ハッシュ値を得る。また、I^0は定数ｋであらわされ、この数値も埋め込み鍵とあわせて秘密とする。

【００３２】トークンの作成において、電子透かし技術によって埋め込まれたＣＦが、一回コピー可能なコンテンツであることを示した場合のみ有効なトークンを付加する。また、電子透かしで埋め込まれたマークから検出した信号からトークンを作り出す。この場合、ユーザー側でのトークンの検証時にも電子透かし検出器からの信号を用いてトークンあるいは要約の作成を行う。

【００３３】作成したトークンは、例えばＭＰＥＧフォーマットのシーケンス・ヘッダ（Sequence header）にある拡張データのユーザ・データ（ＵＤ：User Data）の領域に書き込む。作成されたトークンを非対称鍵を用いてスクランブルして、記録することも可能で、この場合、クラッカーがトークン作成に用いる画像情報の部分を知りえてもトークンを作成することはできない。

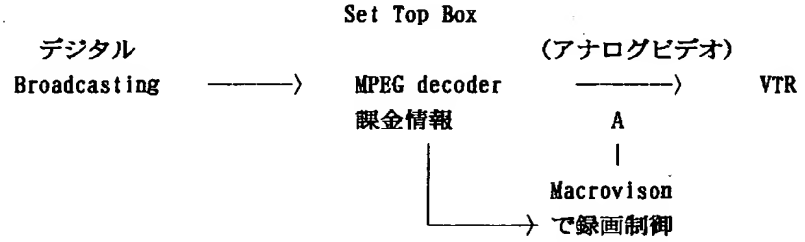
【００３４】ユーザー側では、電子透かし技術によって埋め込まれたＣＦが、一回コピー可能なコンテンツであることを示した場合のみにトークン検証を有効とする。

録画機などで、配信された画像から、同様の方法でトークンを作成しこれが、画像とともに配信されたトークンと一致するか検証する。検証できなければ録画を禁止する。また、ＤＶＤ再生機などのアナログ出力に、アナログ・プロテクション・シグナル（Analog protection signal）やＣＧＭＳ－Ａデータを付加させることによって、アナログへのコピーをも防止する。検証できればトークンを削除または無効化したストリームを、録画させる。（演算結果との非一致を作り出せれば良い）無効化は、トークンに対して行なう。あるいは、画像のうちトークン作成に用いる部分を変更して行なう。（変化後の画像から作成するトークンは、異なったものとなっているので検証が通らない。）さらなる複製を試みようとする場合に、有効なトークンが存在せず、録画が阻止される。トークン付きのコンテンツは、コピーであってはならないので、もし書き換え可能ＤＶＤからのストリームからこれが検出された場合、不正にコピーされたとして、再生を禁止する。

【００３５】図６にディジタル画像配信における複製制御システム方式の、もう１つの実施例として、画像を圧縮した要約から非対称鍵を用いてトークンを作成するシステムを示す。基本的な仕組みは１方向ハッシュ関数を利用した場合と同様である。非対称鍵を用いてトークン＊を作成するシステムの場合に重要な点は、要約からトークンの作成方法は秘密とするが、トークンから要約の作成は公開とする点である。ユーザー側では、録画機などで、配信されたトークンから公開鍵で要約を作り、配信された画像から同様に作成された要約と比較し、一致するか検証する。ＣＦが「1回コピー可」でないのにトークンが有効でも、コピーを禁止する。さらにトークンの無効化を行なう。その他、データ制御に限らず、トークン付加をもって、ある権利を付与し、権利の行使時にトークンの無効化を行なうことで、一度のみの権利行使を認めることができるシステムも同様に実施可能である。例えば電子マネーにトークンをつけておき、支払い時にトークンを無効化する方法も同様に実施できる。

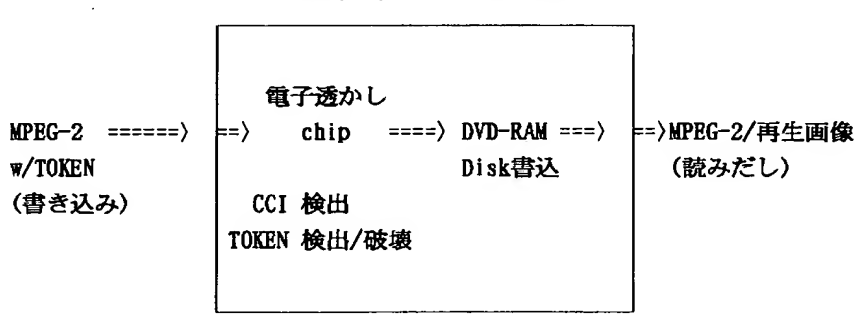
【００３６】次に本発明の応用として、ＳＴＢ内で、簡単な構成で、複製制御を行う方法を説明する。従来、衛星放送等の有料デジタル放送を受信し、課金情報に基づいてアナログ録画の制御を行う方法として Macrovison が存在していた。しかしデジタル信号出力をそのままDVD-RAM等の デジタル recorder に記録することをSTB内で手軽に制御する方法は無かった。以下に Macrovison を使ってアナログ録画を制御する従来の方法を示す。

【００３７】



【００３８】衛星放送等の有料デジタル放送において受信者が料金等を払った時のみデジタル出力の複製許可をSTBの中で簡単に行えるようするには、コントロールフラグとトークンを見ればよい。その理由は以下の通りである。まず、電子透かしで埋め込まれたコントロールフラグを、2bit の Copy Control Information (CCI) と ※し、MPEG-2 stream の User Data Area に入れられたトークン（TOKEN）を検出することにより DVD-RAM等のデジタル Recorderの録画/再生の可否を制御する方法は以下のようになる。

【００３９】



【００４０】ここで書込み、読みだしの各々について、CCI及びトークンの組み合わせによる複製制御の場合分けは以下のようになる。

【００４１】・書込みの場合

CCI/TOKEN	COPY許可
(1,1)	NO COPY
(0,0)	COPY OK

17

(1,0) + TOKEN	COPY OK (書込時TOKEN破壊)
(1,0)	NO COPY
(-,-)	COPY OK

【００４２】・読みだしの場合(DVD-RAMからの場合)

CCI/TOKEN	COPY許可
(1,1)	NO PLAY
(0,0)	PLAY

18

＊(1,0) + TOKEN	NO PLAY
(1,0)	PLAY
(-,-)	PLAY

【００４３】上記より、複製許可をSTBの中で行えるようするには、CCI(1,0) + TOKENを見れば良いことが分かる。

【００４４】

＊

Set Top Box

デジタル Broadcasting ---〉 TOKEN破壊制御 ---〉 デジタル Recorder (MPEG-2) DVD-RAM

A

|

課金情報

【００４５】例えば、デジタル放送において下図のように送出側でCCI(1,0)及びトークンを予め付けておいたMPEG-2 Streamを送出し受信側STBで、外部からの入力情報である、課金情報に基づき、トークンを破壊もしくはそのまま通過させることを制御することによって、DVD-※

(1、0) + TOKEN ---＊---〉TOKEN 破壊 ---〉 NO COPY

＊---〉そのまま通過(TOKEN keep) ---〉 COPY (no more コピー)

※RAM等のデジタル Recorder等、電子透かし検出 chipを持った機器に録画することを制御する方法は以下のようになる。

【００４６】

【００４７】その他、送出側であらかじめトークンをつけるかわりに、トークンに相当する部分に無効なトークンを埋込みSTBで正しいトークンを計算して付加する方 ★

(1、0) + DUMMY TOKEN ---＊---〉そのまま通過(NO TOKEN) --〉 NO COPY

＊---〉TOKEN 付加 ---〉 COPY (no more コピー)

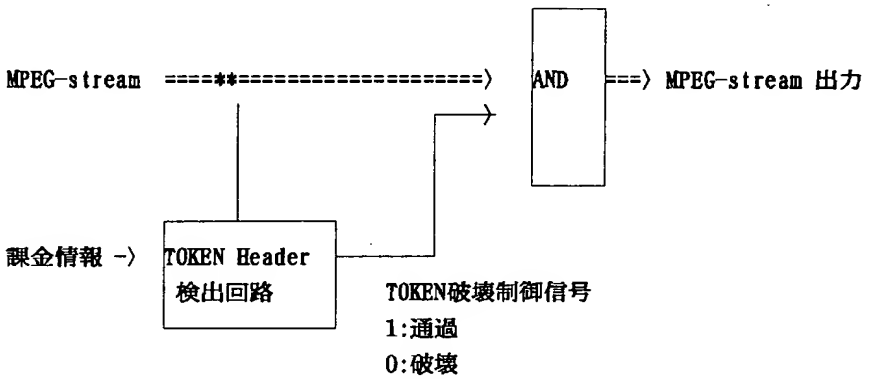
★法を以下に示す。

【００４８】

【００４９】以下、具体的に TOKEN の破壊方法、TOKEN の付加方法を示す。まず TOKEN の破壊方法は、下に示すように MPEG の stream を監視してTOKEN Header を発見する。TOKEN Header が見つかればその後に続くTOK☆

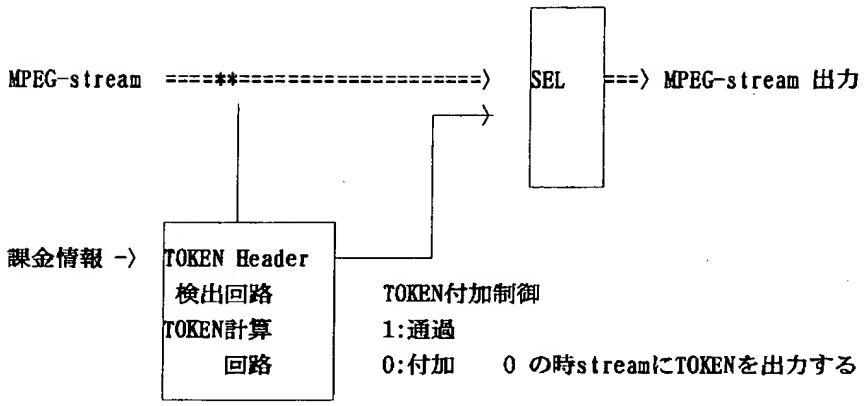
☆ENを破壊するか否かを課金情報を考慮に入れて制御する。TOKEN header 検出回路及びTOKEN破壊のためのAND回路はいずれも容易に構成できる。

【００５０】



【００５１】次に TOKEN の付加方法は、下に示すように MPEG の stream を監視して、Stream から TOKEN を計算、TOKEN Header を発見する。TOKEN Header が見つかればその後に続くTOKEN area(dummy dataが入っている)に課金情報を考慮に入れてTOKENを上書きする。TOKEN header 検出回路及び TOKEN 計算回路及び TOKEN付加のための SELector 回路はいずれも容易に構成できる。

【００５２】



【００５３】上記実施例のように、デジタル放送のSTB等の Consumer Box 内のスマートカードやユーザー課金情報、ユーザー入力情報を元にデジタル映像出力の複製制御(コピー 可、不可)を電子透かしを使って行うための付加情報(TOKEN)の変更がSTB内で容易にできる。ここで重要なことは、STB内で Copy Control Information(CCI)を求める必要がないことである。

【００５４】

【発明の効果】本発明により、配信コンテンツの１回コピーを許可するアプリケーションにおいて、本発明の方法を用いることにより、電子透かし手法をデータ制御のすべてに用いた場合に比べて、機能としては、もとから必要であるＣＦを検出する電子透かし用チップのほかには、トークンを無効にする機能だけですむので、ロジックのゲート数にして約２０分の１以下で、同等かそれ以上の効果を得られる。また、電子透かし技術のみを用いて埋め込んだ場合は、I-frame にしか埋め込みができないため、ＭＰＥＧフォーマットから離れると埋め込んだ複製済みマークが無効になる。一方、本発明の方法では、ＭＰＥＧを離れるとトークンが無効になることは同じであるが、無効になると複製ができないため、複製禁止の効果自体は、データにどの様なフォーマットになっても存続するので、より安全なデータ制御が可能になる。さらに、デジタル放送のSTB等の Consumer Box 内のスマートカードやユーザー課金情報、ユーザー入力情報を元にデジタル映像出力の複製制御を電子透かしを使って行うための付加情報の変更がSTB内で Copy Control Information(CCI)を求める必要なしに、容易に行える。

【図面の簡単な説明】

【図１】データ制御システムのハードウェア構成の一実施例である。

【図２】外付型ＤＶＤドライブを用いたデータ制御システムの概観図である。

【図３】ＤＶＤドライブを内蔵したデータ制御システムの概観図である。

【図４】ＤＶＤ－Ｒデータ制御システムのブロック図である。

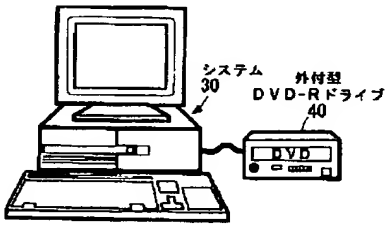
【図５】１方向ハッシュ関数を利用したディジタル画像配信における複製制御システムである。

【図６】非対称鍵を利用したディジタル画像配信における複製制御システムである。

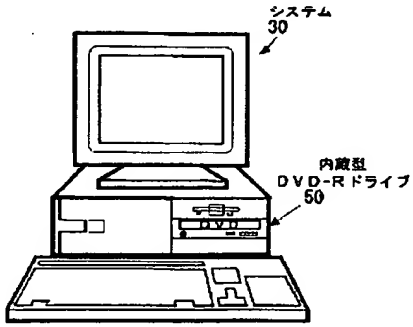
【図７】トークン作成の処理の流れを示す図である。

【図８】データ制御の処理の流れを示す図である。

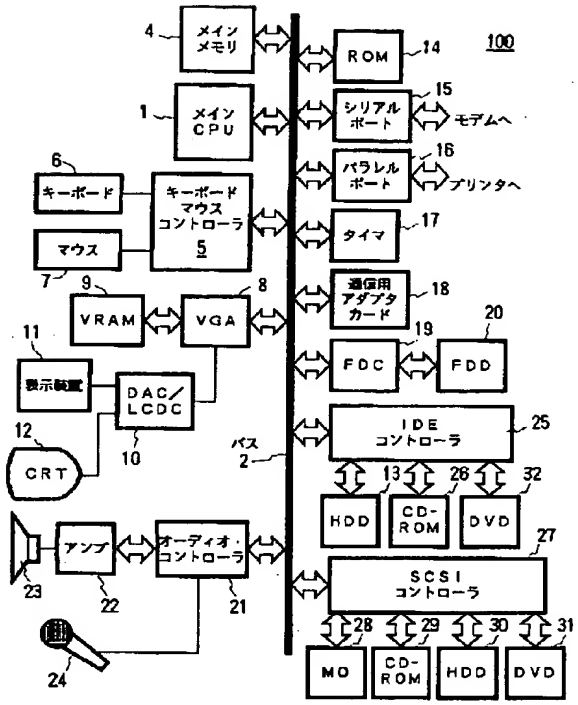
【図２】



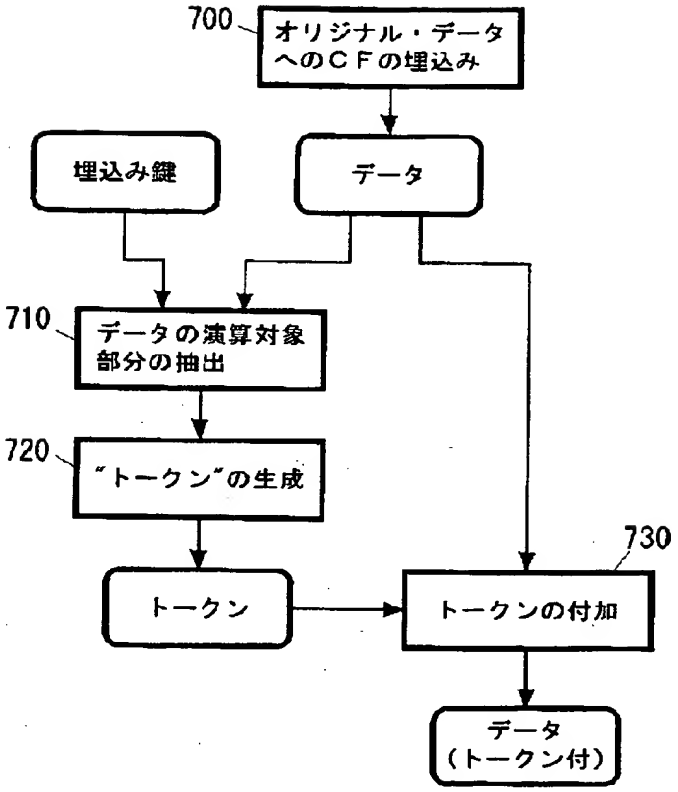
【図３】



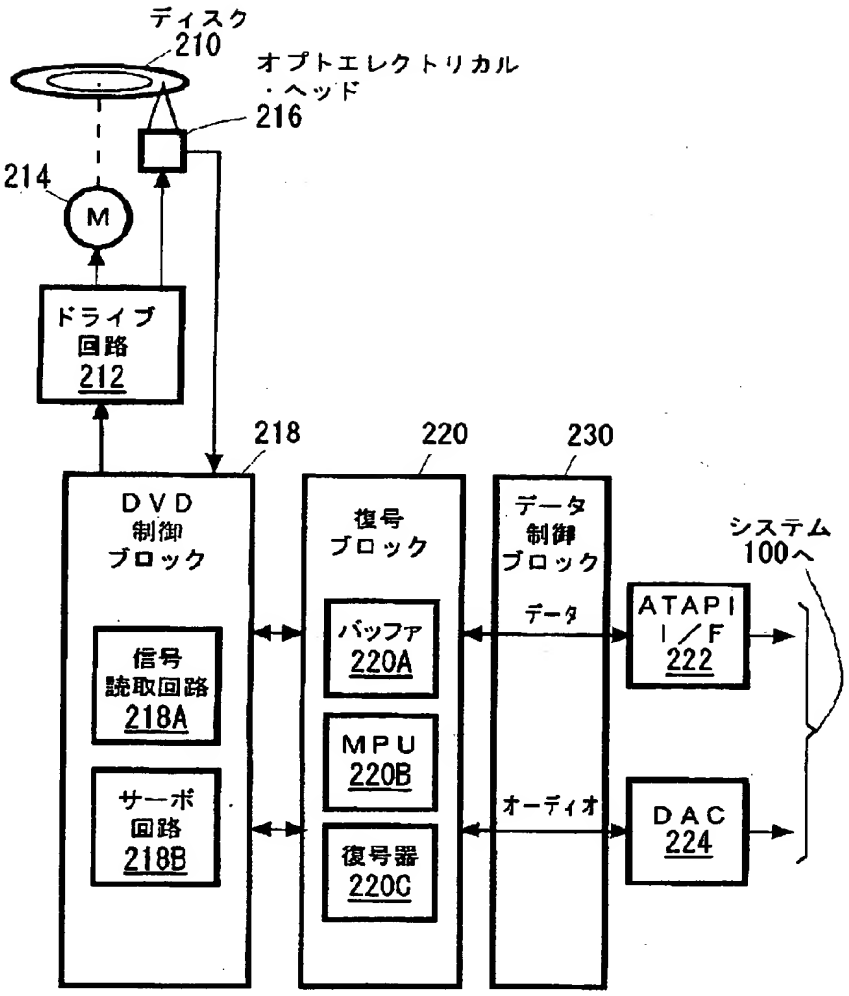
【図１】


4
メイン
メモリ
ROM
14
100
1
メイン
CPU
シリアル
ポート
15
モデムへ
6
キーボード
キーボード
マウス
コントローラ
5
パラレル
ポート
16
プリンタへ
マウス
7
タイマ
17
9
8
VRAM
VGA
通信用
アダプタ
カード
18
11
20
19
FDC
FDD
表示装置
DAC/
LCDC
IDE
コントローラ
25
12
CRT
10
バス
2
13
26
32
HDD
CD-
ROM
DVD
27
アンプ
オーディオ
コントローラ
SCSI
コントローラ
23
22
21
28
29
30
31
MO
CD-
ROM
HDD
DVD
24

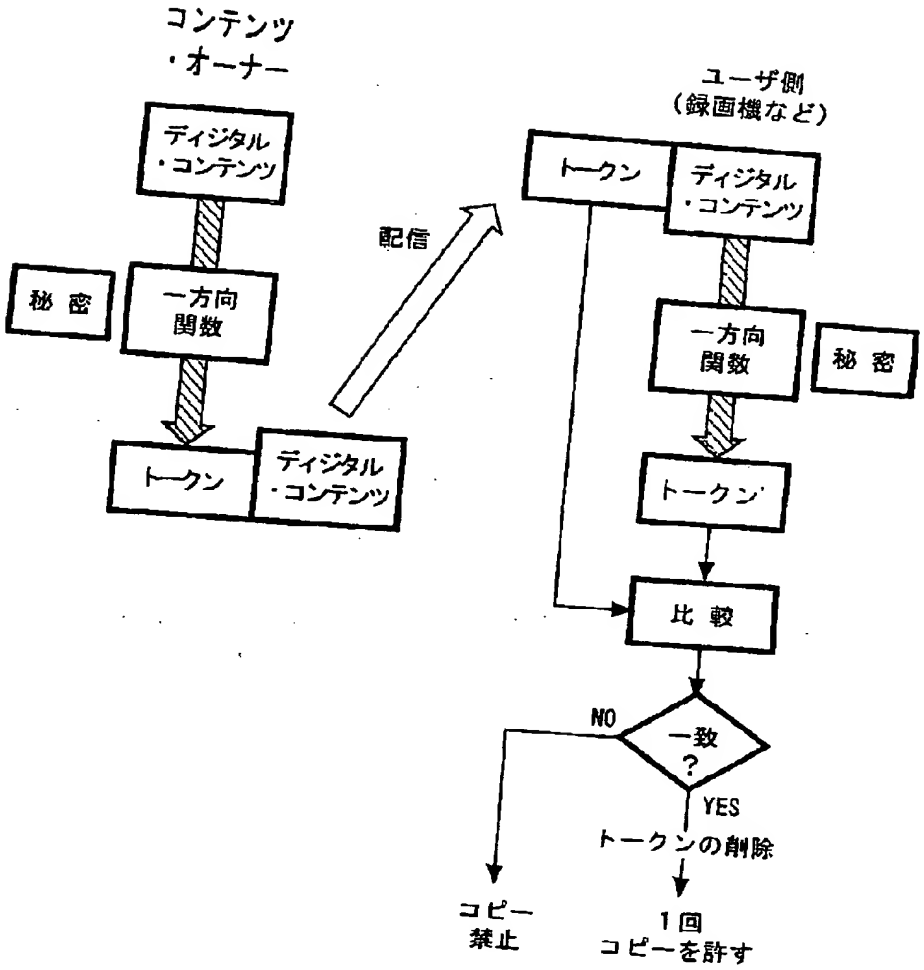
【図７】


700
オリジナル・データ
へのＣＦの埋込み
埋込み鍵
データ
710
データの演算対象
部分の抽出
720
“トークン”の生成
730
トークン
トークンの付加
データ
（トークン付）

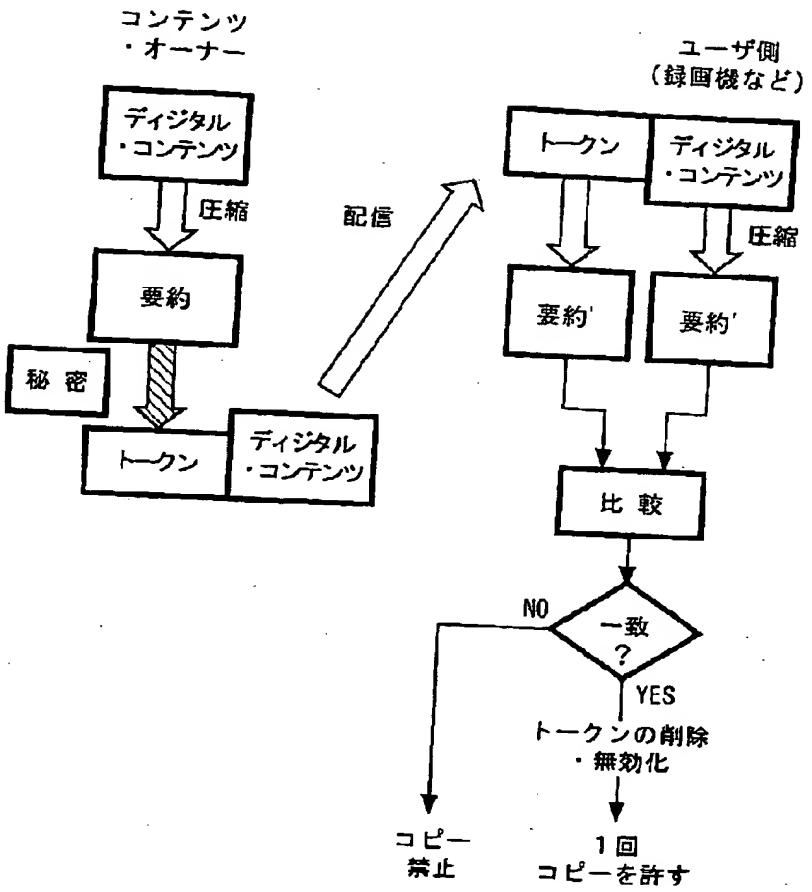
【図4】


ディスク
210
オプトエレクトリカル
・ヘッド
216
214
M
ドライブ
回路
212
218
220
230
DVD
制御
ブロック
信号
読取回路
218A
サーボ
回路
218B
復号
ブロック
バッファ
220A
MPU
220B
復号器
220C
データ
制御
ブロック
データ
オーディオ
ATAPI
I／F
222
DAC
224
システム
100へ

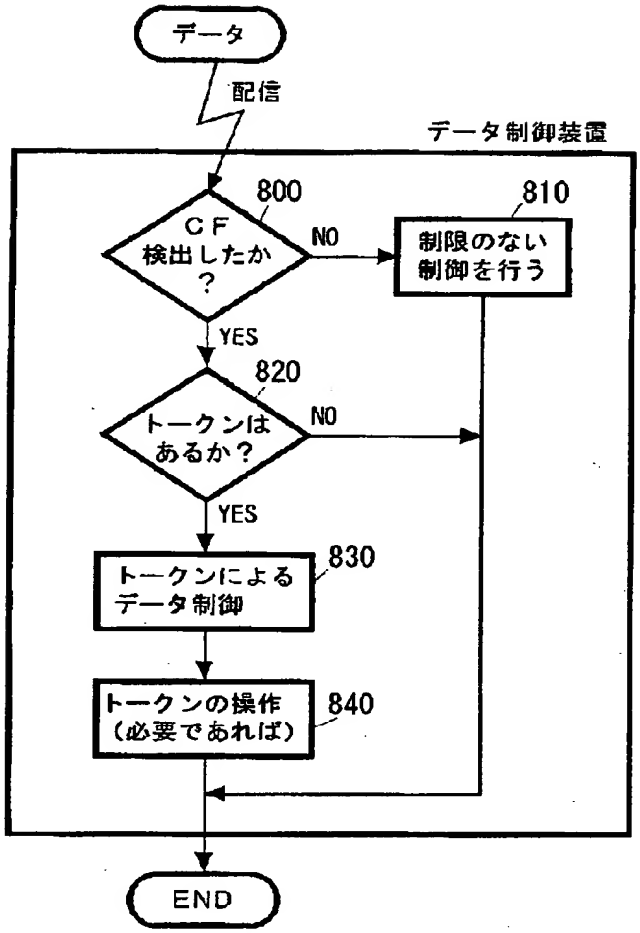
【図5】


コンテンツ
・オーナー
ディジタル
・コンテンツ
秘 密
一方向
関数
トークン
ディジタル
・コンテンツ
配信
ユーザ側
(録画機など)
トークン
ディジタル
・コンテンツ
一方向
関数
秘 密
トークン'
比 較
NO
一致
?
YES
トークンの削除
コピー
禁止
1回
コピーを許す

【図６】


コンテンツ
・オーナー
ディジタル
・コンテンツ
圧縮
要約
秘 密
トークン
ディジタル
・コンテンツ
配信
ユーザ側
（録画機など）
トークン
ディジタル
・コンテンツ
圧縮
要約'
要約'
比 較
NO
一致
？
YES
トークンの削除
・無効化
コピー
禁止
１回
コピーを許す

【図８】



フロントページの続き

(51) Int. Cl.[6]	識別記号	FI	
H04N	7/08	H04N	7/08 Z
	7/081		

(72) 発明者　森本　典繁
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

(72) 発明者　清水　周一
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内